Pacific University
CommonKnowledge

Volume 10 (2010)

Interface: The Journal of Education, Community and Values

6-1-2010

# Cyber War and U.S. Policy: Part I, Neo-realism

Jeffrey Barlow
*Pacific University*

# Cyber War and U.S. Policy: Part I, Neo-realism

**Description**
An editorial based in part on a review of Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco, 2010.

# Cyber War and U.S. Policy: Part I, Neo-realism

Posted on **June 1, 2010** by **Editor**


**Editorial By Jeffrey Barlow**

An editorial based in part on a review of Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco, 2010.

**Introduction:**

"Cyber War" is breaking out on many fronts—at least as a concept for discussion and abundant press coverage. Whether, in fact, it is an emergent form of international conflict and we are fighting one now depends on whom you read, and how they choose to define the concept. We will define it below.

Mike McConnell, a former Vice-Admiral in the U.S. Navy, the former Director of the National Security Agency for the Clinton administration and the Director of National Intelligence for the Bush administration, believes that Cyber War has broken out, and that the United States is losing [1]. The British also believe this is happening, and like McConnell, that the enemy is the Chinese [2]. Very much on the other hand, however, Howard Schmidt, the recently appointed cybersecurity chief for the Obama administration has said: "I think that is a terrible metaphor and I think that is a terrible concept… [3]"

But whether Cyber War is or is not real, and has or has not already begun, policy dealing with it is rapidly being formulated. The just-released (May 28th) *National Security Strategy* of the Obama administration discusses it in some detail [4]. The U.S. has appointed its first "Cyber War General," Lt. General Keith B. Alexander, who also heads the National Security Agency, and the U.S. Air Force has reassigned thirty thousand troops to "the frontlines of Cyber Warfare. [5]"

Clearly, it is important to examine the concept of Cyber War in some detail. We have argued at *Interface* that the concept of Cyber War as currently used is so broad that it is of little value [6].

Recently, two highly respected authorities with a great deal of clout as policy analysts have examined the concept and discussed appropriate policy in a new work, *Cyber War: The Next Threat to National Security and What to Do About It*. Richard A. Clarke, the primary author, was prominent in counter-terrorism and particularly in Cybersecurity for both the Clinton and Bush administrations, and his co-author, Robert Knake, a member of the Council on Foreign Relations also has a considerable history of writing and speaking about Cyber War [7].

This work is very welcome because Clarke and Knake give us a very straightforward and usefully limited definition of Cyber War which carefully excludes much of the Chicken Little gabble often found in the popular press: "When the term "Cyber War" is used in this book, it refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. [8]" That cautious sentence alone makes the book worthwhile and we expect that it will dominate academic and policy discussions for some time, on the order of Herman Kahn's 1960 work, *On Thermonuclear War*, which defined many of the policy issues around nuclear war [9]. *Cyber War: The Next Threat to National Security and What to Do About It* may in fact be responsible for some of the recent developments we discussed above, such as the creation of the new cyber commands.

This piece is not a review of Clarke and Knake's work, but a start at laying out the various schools of thought on the issues around Cyber War. We utilize it as a scaffold here because of its lucidity, its highly organized development, and its approach, which places Cyber War into a historical context which gives many useful insights into what might be appropriate policies. At the same time, we recognize that many other authorities, or at least highly influential figures, like Mike McConnell mentioned above, disagree, and will cover their positions in Part II of this editorial, to be published in August at *Interface*.

**Neorealist views of Cyber War:**

Clarke and Knake's theoretical orientation is what policy wonks would call "Neorealist" [10]. The Neorealist position has been intellectually powerful and its policies have arguably prevented nuclear war, the potential ultimate breakdown of the international order, since 1945. It is the history of this position and its contributions to preventing nuclear war which make it a useful place to begin analyzing Cyber War.

The Neorealists, like the classical Realists, see the world as an inherently dangerous place as states inevitably must compete for power in a disorderly international system. But the Neorealists believe that threat of instability can best be constrained by a stable world order in which a small number of powerful states (ideally two—a bi-polar structure, the classic example being the world of the Cold War) limit potential conflict out of self-interest. Particularly important to such stability is open communications and as many agreements and treaties as can be signed.

However, although the development of the concept of Cyber War promises to be fully as threatening and destabilizing to the world order as was nuclear war, the two are obviously quite

different. Cyber War presents a number of new challenges to the international order, and to both Realism and Neorealism.

For example, there was never going to be any doubt as to the question of whether or not nuclear war had occurred, nor very little as to who was responsible. But cyber assets are non-physical and there are many ways to attack them unobserved, or at least un-identified. When Japanese forces attacked Pearl Harbor, the situation was easily understood; attacks on an enemy's military assets have often been a cause of war. But it is not always clear how to detect an opening skirmish in Cyber War.

Cyber battles then, are always going to have important elements of ambiguity. For example, in 2009 when somebody, perhaps acting from China, hacked into a defense contractor's computer and stole the plans for a radically new U.S. fighter plane, the F-35 [11], was this an act of war, of espionage, or of commercial piracy? [12] What was an appropriate response and against whom should any counter attack be launched?

If Cyber War is elusive, however, Clarke and Knake demonstrate that it is nonetheless real, and presents an imminent danger. Moreover, the United States, they believe, is woefully unprepared to create appropriate policies to help maintain stability in a world in which minor states, even criminal gangs or politically-motivated individuals, have the power to launch a devastating attack against a great nation.

We are, of course, discussing a form of violence markedly below the attacks on Hiroshima and Nagasaki, but Clarke and Knake present a number of terrifying possibilities:

*"If they take over a network, cyber warriors could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send a platoon into an ambush, or cause a missile to detonate in the wrong place. If Cyber Warriors crash networks, wipe out data, and turn computers into doorstops, then a financial system could collapse, a supply chain could halt, a satellite could spin out of orbit into space, an airline could be grounded. These are not hypotheticals. Things like this have already happened, sometimes experimentally, sometimes by mistake, and sometimes as a result of cyber crime or cyber war. [13]"*

From these examples, the authors try to evolve appropriate Neorealist policy responses. Here again Neorealist precedents began to break down, because, as the authors point out, Cyber Warfare capabilities are highly asymmetrical. Cyber War is more similar to terrorism or guerrilla warfare in that regard than to classical set-piece battles or nuclear exchanges.

The United States has an unsurpassed offensive capability in "kinetic warfare," the traditional form of war in which one side launches metal or explosives at the other from various platforms ranging from a compound bow to a nuclear missile. Kinetic war has usually depended upon economic power. The United States outspends the rest of the world put together on kinetic

weapons. But Cyber War enables very weak states, which are in every other regard basket cases, to wreak great damage, perhaps without even being caught doing so.

As in kinetic warfare, the U.S. has unparalleled advantages in offensive Cyber War because of its technological base. But, unfortunately, it also has one of the weakest defenses against Cyber War of any nation. It simply has too much to defend and there has been little or no planning or coordination in protecting the vast American complex of digital systems.

Warfare has always proceeded as a sort of on-going struggle between defense and offense. Nuclear weapons permitted no real defense; offense has been king since August 1945. The ultimate Neorealist peacekeeping strategy since than has been to ensure not that one could survive an attack, but that no aggressor could survive a counter-attack. It was on that calculus that cold-war treaties and agreements were founded.

But Cyber War again is different. Presuming some minimal level of investment, even in off-the-shelf technologies available on line from hundreds of sources, very weak states, terrorist groups, and even individuals, potentially have offensive capabilities.

Given that minimal offensive ability, the economically less developed a potential aggressor is, the better its inherent defenses. North Korea accordingly has powerful offensive capability and a very strong defense—dire poverty; it has very little to "take down." States with offensive Cyber War capabilities include not only unified Europe, rising China, and a renascent Russia, but also many very minor powers like North Korea.

The most powerful potential enemy, in the judgment of the authors, is first Russia, then China. Each of these brings special advantages to Cyber War. The Russian government might be said to have great offensive power; it has access to the most sophisticated hacker gangs in the world [14], and in some cases seemingly overlaps with them.

The Chinese state, too, has a superior potential offense. It, according to Clarke, has trained thousands of civilian Cyber Warriors [15], particularly among patriotic Chinese youth, markedly expanding the already very high capabilities of China's formal military forces. Defensively, they have such control over their own Internet that if they chose to "go first" in a Cyber War, they could simultaneously disengage from the global Internet, markedly reducing retaliatory action from others.

Part of the undeniable hysteria over Cyber War then, is the dawning realization that under the impact of the Internet, very important balances have changed. The United States, long dominant in kinetic warfare, may be critically behind in an important emerging form of combat.

In the Neorealist perspective, lacking a strong defense, what is a nation like the U.S. to do to ward off cyber attacks? At present our strategy consists of the Old Time Religion of warfare, threatening to "go kinetic". That is, if you do marked cyber damage to us, we bomb, perhaps

even nuke, you. Clarke and Knake lay out the policy alternatives thusly:

*"If we do not have a credible defense strategy, we will be forced to escalate in a cyber conflict very quickly. We will need to be more aggressive in getting our adversary's systems so that we can stop their attacks before they reach our undefended systems. That will be destabilizing, forcing us to treat potential adversaries as current ones. We will also need to take a stronger declaratory posture to try to deter attacks on our systems by threatening to "go kinetic" in response to a cyber attack, and it will be more likely that our adversaries will think they can call that bluff. [16]"*

Clarke and Knake think this a momentarily necessary policy, but ultimately limited.

Clarke is deeply suspicious of those in the American military who draw quick comparisons to past war-fighting technologies in which cyber space is viewed simply as another battlefield:

*"...the U.S. military in general repeatedly characterizes cyberspace as something to be dominated. It is reminiscent of the Pentagon's way of speaking of nuclear war in the 1960s. The historian of nuclear strategy Lawrence Freedman noted that William Kaufmann, Henry Kissinger, and other strategists realized that there was a need then "to calm the spirit of offense, potent in Air Force circles...[whose] rhetoric encouraged a view of war that was out-moded and dangerous." That same sort of macho rhetoric is strong in Air Force cyber war circles today, and apparently in the Navy as well [17]."*

**Conclusion: Neorealism Fails?**

The Neorealist framework of Clarke and Knake gives their concept of Cyber War great resonance. Many of their analogies place it into a deceptively familiar framework, that of the post-war era dominated by kinetic technology. Accordingly, the reception of this book has been overwhelmingly positive [18]; some think it almost prophetic. Clarke, of course, is an ideal candidate for Prophet, at least among policy wonks, having repeatedly attempted to draw the incoming Bush administration's attention to the dangers presented by Bin Laden well in advance of the 9/11 catastrophe. He was, however, largely ignored.

When we survey Clarke and Knake's Neorealist policy prescriptions, we get some insight into how it was that, despite Clarke's prescience prior to 9/11, his dire warnings went unheeded. The authors propose actions that would require creating a new political order, internally and externally. They call for vast changes in the relationships between peoples and their governments, and between all governments, worldwide. Internationally, a whole new series of treaties and organizations would be necessary. These sweeping calls for action render the authors very vulnerable to critics.

The greatest fear and the worst weakness of Neorealist strategic thinking with regard to nuclear war, however, was always simply that things would get out of control either through accident or

miscalculation. This weakness makes Neorealist solutions even less likely to succeed in preventing cyber conflicts.

There are too many differences between kinetic war, especially nuclear war, and Cyber War. Neorealism depends on a limited number of rational actors who work together to restrain violence. The potential theater of Cyber War is global; the potential aggressors, legion.

The problem of attribution is itself ultimately unsolvable given current technologies. There are too many ways for an attacker to cloak his or her identity, or worse, to spoof it—lay electronic trails to another—so that a misattribution occurs, resulting in a cyber equivalent of an erroneous counter-strike which would truly result in Cyber War [19].

But even if the problem of misattribution were solved, there are simply too many players and too many conflicting ideologies. Some of these are so non-materialist—and hence in an important sense irrational, unconfined by the bounds of reason alone—as to render their adherents totally disinterested in stability.

We think then, that the Neorealist model holds out little prospect of preventing Cyber War, even if Clarke and Knake nonetheless believe it to be the best hope. Even if Neorealist prescriptions, that is, a system of treaties and agreements buttressed by increasing attention to defense in the case of the United States [20], offers some hope of eventual security in a world in which Cyber War is a real possibility, it also presages an extended period of what might well be termed "Cold Cyber War". This may well be marked by continual conflicts which all sides hope can be contained to something less than the Cyber War equivalent of nuclear strikes. Here the Neorealist program offers some ameliorative policies. Certainly the more agreements that are arrived at, the better we will all understand the important issues, if nothing else.

We will present opposing views to Neorealism as represented by Clarke and Knake and discuss such criticisms in Part II of this series, to be published in August. Many of these are, we believe, classically "Realist" and posit a world of endless struggle, for the near future marked by continual Cyber conflicts.

**Endotes**

[1] See McConnell's article which has driven much of the furor at: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/ AR2010022502493.html

[2] See Michael Evans, Giles Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets" in *The Times Online*, March 8, 2010 at: http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053254 .ece

[3] Ryan Singel, "White House Cyber Czar: 'There Is No Cyberwar' at: http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

[4] Download the full PDF document from: http://www.whitehouse.gov/blog/2010/05/27/a-blueprint-pursuing-world-we- seek While cyber security is discussed throughout, see especially page 27 in this version of the document.

[5] See Peter Beaumont, "US appoints first Cyber Warfare general, *The Guardian*, May 23, 2010 at: http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare- general

[6] See "Cyber War or Cyber Vigilantism?" at: http://bcis.pacificu.edu/journal/2010/03/article.php?id=660

[7] See his pages at the Council at: http://www.cfr.org/bios/15502/robert_k_knake.html

[8] Highlight Loc. 186-92 (Kindle edition)

[9] There is a commendably brief analysis of the book with good attributions found at: http://en.wikipedia.org/wiki/On_Thermonuclear_War

[10] The earlier Realist school evolved into the Neorealist position. There is an excellent Wikipedia page (because carefully written and very well founded in appropriate research) to be found at: http://en.wikipedia.org/wiki/Political_realism The Realists believe that all states are inherently competitive, must ultimately depend on their own forces for security, and that attempts to restrain violence through international organizations or agreements are ultimately naïve. The Neorealist position is defined below in the text.

[11] See: Siobhan Gorman, August Cole, Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009, at http://online.wsj.com/article/SB124027491029837401.html

[12] Clarke and Knake, – Highlight Loc. 2601-8 Kindle edition. Those following up source materials in a Kindle edition are aware, of course, that these can vary somewhat depending on various settings, though they should be close to the location I have marked here. I assume this to be even truer if the work were read on another brand of electronic reader, but am not certain that it is.

[13] Highlight Loc. 1091-95 (Kindle edition)

[14] See our review of Joseph Menn's work, *Fatal System Error*, at: http://bcis.pacificu.edu/journal/2010/02/article.php?id=648

[15] While it is irrelevant here, I personally find this perspective overstated. I do not believe the relationship between the Chinese state and the Patriotic Youth hackers to be that formal, though it is clearly a useful one to the state, however loosely organized it may be.

[16] Highlight Loc. 2367-71

[17] Highlight Loc. 689-95

[18] See the review of Clarke and Knake at "Armageddon Online" at: http://www.armageddononline.org/cyber-attack-electronic-pearl-harbor. html

[19] Some of what are often thought to be Russian Cyber War attacks on break-away political interests, for example, were launched from enslaved botnets in the United States. The electronic trail of the recent violations of Google accounts in China led first to Taiwan, then to the United States, then onto China. Given the unwillingness of Chinese authorities to open up their servers to foreign scrutiny there is no real certainty that the trail ended there.

[20] This is my own reading of the underlying intent of the "National Security Strategy" referred to above.

This entry was posted in Uncategorized by **Editor**. Bookmark the **permalink [http://bcis.pacificu.edu/interface/?p=3797]** .

11 THOUGHTS ON "CYBER WAR AND U.S. POLICY: PART I, NEO-REALISM"

**nigeria**
on **January 30, 2014 at 1:55 PM** said:

One additional issue I want to talk about is that as an selection to trying to accommodate all your on the net degree lessons on times that you end work (since the majority people are tired after they get home), try to get most of one's instructional classes on the week-ends and only a couple courses in weekdays, even if it ways a tiny time away through the saturday and sunday. This can be good because on the saturdays and sundays, you are additional rested along with concentrated in school work. Thanks significantly to your numerous issues I have figured out from your site.

**selfinger.com**
on **January 30, 2014 at 2:16 PM** said:

Hey would you mind letting me know which hosting company you're utilizing?

I've loaded your blog in 3 completely different web browsers and I must say this blog loads a lot

quicker then most. Can you suggest a good hosting provider at a reasonable price? Cheers, I appreciate it!

**Tad Young**
on **January 30, 2014 at 6:17 PM** said:

Great beat ! I would like to apprentice whilst you amend your website, how can i subscribe for a blog site? The account aided me a acceptable deal. I had been a little bit familiar of this your broadcast provided brilliant clear concept

**ray ban sale**
on **February 1, 2014 at 1:44 AM** said:

There's nothing ever before sublte with regards to the Medusa trade name. This situation trade name, started because of developer Gianni Ray ban sunglasses in less than 1937, is roughly captivating, captivating and so enchanting European-style, The idea further suggests a good undisputable irreverent rock-star perspective.

**plotka**
on **February 1, 2014 at 1:48 AM** said:

We are a group of volunteers and commencing a new scheme in our community. Your website provided us with valuable facts to paintings on. You have performed an impressive career and our entire neighborhood can also be thankful to you.

**motoryzacja**
on **February 1, 2014 at 2:17 AM** said:

Thanks for your advice! I am going to read it to realize far more about Holy Cross.

**http://healthclever.jigsy.com**
on **February 2, 2014 at 3:09 PM** said:

Browsing this info made it easier for me to figure out a good number of things I was ignorant of!

**garlic allicin**
on **February 2, 2014 at 3:14 PM** said:

Please keep writing such great info, I like this kind of articles!

**9ja**
on **February 3, 2014 at 1:43 AM** said:

Great blog right here! Additionally your site loads up incredibly fast! What host are you the usage of? Can I get your associate link on your host? I wish my internet site loaded up as quickly as yours lol

**plotki**
on **February 3, 2014 at 1:56 AM** said:

This really answered my drawback, thank you!

**nigeria dating**
on **February 5, 2014 at 12:17 AM** said:

I also, want a followup to this repair. It's fasinating. I after had a repair made over a cast iron exhaust manifold for just a 1932 Packard.